



# Configuring SSH and Telnet

---

This chapter contains the following sections:

- [Information About SSH and Telnet, on page 1](#)
- [Guidelines and Limitations for SSH, on page 3](#)
- [Configuring SSH, on page 3](#)
- [Configuration Examples for SSH, on page 10](#)
- [Configuring X.509v3 Certificate-Based SSH Authentication, on page 12](#)
- [Configuration Example for X.509v3 Certificate-Based SSH Authentication, on page 14](#)
- [Configuring Telnet, on page 15](#)
- [Verifying the SSH and Telnet Configuration, on page 17](#)
- [Default Settings for SSH, on page 18](#)

## Information About SSH and Telnet

### SSH Server

The Secure Shell Protocol (SSH) server feature enables a SSH client to make a secure, encrypted connection to a Cisco Nexus device. SSH uses strong encryption for authentication. The SSH server in the Cisco Nexus device switch interoperates with publicly and commercially available SSH clients.

The user authentication mechanisms supported for SSH are RADIUS, TACACS+, and the use of locally stored user names and passwords.

### SSH Client

The SSH client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a switch to make a secure, encrypted connection to another Cisco Nexus device or to any other device running an SSH server. This connection provides an outbound connection that is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco Nexus device works with publicly and commercially available SSH servers.

## SSH Server Keys

SSH requires server keys for secure communications to the Cisco Nexus device. You can use SSH keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algorithm (DSA)

Be sure to have an SSH server key-pair with the appropriate version before enabling the SSH service. You can generate the SSH server key-pair according to the SSH client version used. The SSH service accepts three types of key-pairs for use by SSH version 2:

- The `dsa` option generates the DSA key-pair for the SSH version 2 protocol.
- The `rsa` option generates the RSA key-pair for the SSH version 2 protocol.

By default, the Cisco Nexus device generates an RSA key using 1024 bits.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)



---

**Caution** If you delete all SSH keys, you can't start the SSH services.

---

## SSH Authentication Using Digital Certificates

SSH authentication on CiscoNX-OS devices provide X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is signed by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through a query or a notification. Verification of certificates is successful if the certificates are from any of the trusted CAs.

You can configure your device for SSH authentication using an X.509 certificate. If the authentication fails, you are prompted for a password.

You can configure SSH authentication using X.509v3 certificates (RFC 6187). X.509v3 certificate-based SSH authentication uses certificates combined with a smartcard to enable two-factor authentication for Cisco device access. The SSH client is provided by Cisco partner Pragma Systems.

## Telnet Server

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site, and then passes the keystrokes from one system to the other. Telnet can accept either an IP address or a domain name as the remote system address.

The Telnet server is enabled by default on the Cisco Nexus device.

## Guidelines and Limitations for SSH

SSH has the following configuration guidelines and limitations:

- The Cisco Nexus device supports only SSH version 2 (SSHv2).
- SSH public and private keys imported into user accounts that are remotely authenticated through a AAA protocol (such as RADIUS or TACACS+) for the purpose of SSH Passwordless File Copy will not persist when the Nexus device is reloaded unless a local user account with the same name as the remote user account is configured on the device before the SSH keys are imported.

## Configuring SSH

### Generating SSH Server Keys

You can generate an SSH server key based on your security requirements. The default SSH server key is an RSA key that is generated using 1024 bits.

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ssh key {dsa [force] | rsa [bits [force]]}**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh key [dsa | rsa] [md5]**
5. (Optional) switch# **copy running-config startup-config**

#### DETAILED STEPS

##### Procedure

|               | Command or Action                                                 | Purpose                                                                                                                                                                                                                                    |
|---------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                 | Enters global configuration mode.                                                                                                                                                                                                          |
| <b>Step 2</b> | switch(config)# <b>ssh key {dsa [force]   rsa [bits [force]]}</b> | Generates the SSH server key.<br><br>The <i>bits</i> argument is the number of bits used to generate the key. The range is from 768 to 4096 and the default value is 1024.<br><br>Use the <b>force</b> keyword to replace an existing key. |
| <b>Step 3</b> | switch(config)# <b>exit</b>                                       | Exits global configuration mode.                                                                                                                                                                                                           |
| <b>Step 4</b> | (Optional) switch# <b>show ssh key [dsa   rsa] [md5]</b>          | Displays the SSH server keys.                                                                                                                                                                                                              |

|               | Command or Action                                            | Purpose                                                                                                                                                                                                                                                                                                                         |
|---------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                              | For Cisco NX-OS Release 7.0(3)I4(6) and any later 7.0(3)I4(x) release, this command displays the fingerprint in SHA256 format by default. SHA256 is more secure than the old default format of MD5. However, the <b>md5</b> option has been added, if you want to see the fingerprint in MD5 format for backward compatibility. |
| <b>Step 5</b> | (Optional) switch# <b>copy running-config startup-config</b> | Copies the running configuration to the startup configuration.                                                                                                                                                                                                                                                                  |

### Example

The following example shows how to generate an SSH server key:

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

## Specifying the SSH Public Keys for User Accounts

You can configure an SSH public key to log in using an SSH client without being prompted for a password. You can specify the SSH public key in one of three different formats:

- Open SSH format
- IETF SECSH format
- Public Key Certificate in PEM format

### Specifying the SSH Public Keys in Open SSH Format

You can specify the SSH public keys in SSH format for user accounts.

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **username** *username* **sshkey** *ssh-key*
3. switch(config)# **exit**
4. (Optional) switch# **show user-account**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|               | Command or Action                                                            | Purpose                                                        |
|---------------|------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                            | Enters global configuration mode.                              |
| <b>Step 2</b> | switch(config)# <b>username</b> <i>username</i> <b>sshkey</b> <i>ssh-key</i> | Configures the SSH public key in SSH format.                   |
| <b>Step 3</b> | switch(config)# <b>exit</b>                                                  | Exits global configuration mode.                               |
| <b>Step 4</b> | (Optional) switch# <b>show user-account</b>                                  | Displays the user account configuration.                       |
| <b>Step 5</b> | (Optional) switch# <b>copy running-config startup-config</b>                 | Copies the running configuration to the startup configuration. |

### Example

The following example shows how to specify an SSH public key in open SSH format:

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4WlAV9Y2t2hrEWgbUEYz
CfTP05B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rzZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnXlbvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```



**Note** The **username** command in the example above is a single line that has been broken for legibility.

## Specifying the SSH Public Keys in IETF SECSH Format

You can specify the SSH public keys in IETF SECSH format for user accounts.

### SUMMARY STEPS

1. switch# **copy server-file bootflash:** *filename*
2. switch# **configure terminal**
3. switch(config)# **username** *username* **sshkey file** *filename*
4. switch(config)# **exit**
5. (Optional) switch# **show user-account**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|               | Command or Action                                                                  | Purpose                                                                                                                     |
|---------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>copy</b> <i>server-file</i> <b>bootflash:</b> <i>filename</i>           | Downloads the file that contains the SSH key in IETF SECSH format from a server. The server can be FTP, SCP, SFTP, or TFTP. |
| <b>Step 2</b> | switch# <b>configure terminal</b>                                                  | Enters global configuration mode.                                                                                           |
| <b>Step 3</b> | switch(config)# <b>username</b> <i>username</i> <b>sshkey file</b> <i>filename</i> | Configures the SSH public key in SSH format.                                                                                |
| <b>Step 4</b> | switch(config)# <b>exit</b>                                                        | Exits global configuration mode.                                                                                            |
| <b>Step 5</b> | (Optional) switch# <b>show user-account</b>                                        | Displays the user account configuration.                                                                                    |
| <b>Step 6</b> | (Optional) switch# <b>copy running-config startup-config</b>                       | Copies the running configuration to the startup configuration.                                                              |

### Example

The following example shows how to specify the SSH public key in the IETF SECSH format:

```
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

## Specifying the SSH Public Keys in PEM-Formatted Public Key Certificate Form

You can specify the SSH public keys in PEM-formatted Public Key Certificate form for user accounts.

### SUMMARY STEPS

1. switch# **copy** *server-file* **bootflash:** *filename*
2. switch# **configure terminal**
3. (Optional) switch# **show user-account**
4. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|               | Command or Action                                            | Purpose                                                                                                                                            |
|---------------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>copy server-file bootflash: filename</b>          | Downloads the file that contains the SSH key in PEM-formatted Public Key Certificate form from a server. The server can be FTP, SCP, SFTP, or TFTP |
| <b>Step 2</b> | switch# <b>configure terminal</b>                            | Enters global configuration mode.                                                                                                                  |
| <b>Step 3</b> | (Optional) switch# <b>show user-account</b>                  | Displays the user account configuration.                                                                                                           |
| <b>Step 4</b> | (Optional) switch# <b>copy running-config startup-config</b> | Copies the running configuration to the startup configuration.                                                                                     |

### Example

The following example shows how to specify the SSH public keys in PEM-formatted public key certificate form:

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

## Configuring the SSH Source Interface

You can configure SSH to use a specific interface.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip ssh source-interface type slot/port**
3. switch(config)# **show ip ssh source-interface**

### DETAILED STEPS

#### Procedure

|               | Command or Action                                             | Purpose                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                             | Enters global configuration mode.                                                                                                                                                                                         |
| <b>Step 2</b> | switch(config)# <b>ip ssh source-interface type slot/port</b> | Configures the source interface for all SSH packets. The following list contains the valid values for <i>interface</i> . <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> </ul> |

|               | Command or Action                                   | Purpose                                                                          |
|---------------|-----------------------------------------------------|----------------------------------------------------------------------------------|
|               |                                                     | <ul style="list-style-type: none"> <li>• port-channel</li> <li>• vlan</li> </ul> |
| <b>Step 3</b> | switch(config)# <b>show ip ssh source-interface</b> | Displays the configured SSH source interface.                                    |

### Example

This example shows how to configure the SSH source interface:

```
switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip ssh source-interface ethernet 1/7
switch(config)# show ip ssh source-interface
VRF Name                               Interface
default                                 Ethernet1/7
```

## Starting SSH Sessions to Remote Devices

You can start SSH sessions to connect to remote devices from your Cisco Nexus device.

### SUMMARY STEPS

1. switch# **ssh** {hostname | username@hostname} [**vrf** vrf-name]

### DETAILED STEPS

#### Procedure

|               | Command or Action                                                        | Purpose                                                                                                       |
|---------------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>ssh</b> {hostname   username@hostname} [ <b>vrf</b> vrf-name] | Creates an SSH session to a remote device. The <i>hostname</i> argument can be an IPv4 address or a hostname. |

## Clearing SSH Hosts

When you download a file from a server using SCP or SFTP, you establish a trusted SSH relationship with that server.

### SUMMARY STEPS

1. switch# **clear ssh hosts**



**DETAILED STEPS****Procedure**

|               | Command or Action              | Purpose                       |
|---------------|--------------------------------|-------------------------------|
| <b>Step 1</b> | switch# <b>clear ssh hosts</b> | Clears the SSH host sessions. |

**Disabling the SSH Server**

By default, the SSH server is enabled on the Cisco Nexus device.

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **[no] feature ssh**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh server**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS****Procedure**

|               | Command or Action                                            | Purpose                                                        |
|---------------|--------------------------------------------------------------|----------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                            | Enters global configuration mode.                              |
| <b>Step 2</b> | switch(config)# <b>[no] feature ssh</b>                      | Enables/disables the SSH server. The default is enabled.       |
| <b>Step 3</b> | switch(config)# <b>exit</b>                                  | Exits global configuration mode.                               |
| <b>Step 4</b> | (Optional) switch# <b>show ssh server</b>                    | Displays the SSH server configuration.                         |
| <b>Step 5</b> | (Optional) switch# <b>copy running-config startup-config</b> | Copies the running configuration to the startup configuration. |

**Deleting SSH Server Keys**

You can delete SSH server keys after you disable the SSH server.



**Note** To reenable SSH, you must first generate an SSH server key.

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**

3. switch(config)# **no ssh key [dsa | rsa]**
4. switch(config)# **exit**
5. (Optional) switch# **show ssh key**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### Procedure

|               | Command or Action                                            | Purpose                                                                   |
|---------------|--------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                            | Enters global configuration mode.                                         |
| <b>Step 2</b> | switch(config)# <b>no feature ssh</b>                        | Disables the SSH server.                                                  |
| <b>Step 3</b> | switch(config)# <b>no ssh key [dsa   rsa]</b>                | Deletes the SSH server key.<br>The default is to delete all the SSH keys. |
| <b>Step 4</b> | switch(config)# <b>exit</b>                                  | Exits global configuration mode.                                          |
| <b>Step 5</b> | (Optional) switch# <b>show ssh key</b>                       | Displays the SSH server configuration.                                    |
| <b>Step 6</b> | (Optional) switch# <b>copy running-config startup-config</b> | Copies the running configuration to the startup configuration.            |

## Clearing SSH Sessions

You can clear SSH sessions from the Cisco Nexus device.

### SUMMARY STEPS

1. switch# **show users**
2. switch# **clear line vty-line**

## DETAILED STEPS

### Procedure

|               | Command or Action                  | Purpose                            |
|---------------|------------------------------------|------------------------------------|
| <b>Step 1</b> | switch# <b>show users</b>          | Displays user session information. |
| <b>Step 2</b> | switch# <b>clear line vty-line</b> | Clears a user SSH session.         |

## Configuration Examples for SSH

The following example shows how to configure SSH:

**SUMMARY STEPS**

1. Generate an SSH server key.
2. Enable the SSH server.
3. Display the SSH server key.
4. Specify the SSH public key in Open SSH format.
5. Save the configuration.

**DETAILED STEPS****Procedure**

**Step 1** Generate an SSH server key.

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

**Step 2** Enable the SSH server.

```
switch# configure terminal
switch(config)# feature ssh
```

**Note**

This step should not be required because the SSH server is enabled by default.

**Step 3** Display the SSH server key.

```
switch(config)# show ssh key
rsa Keys generated:Fri May 8 22:09:47 2009

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGs7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024
fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*****
could not retrieve dsa key information
*****
```

**Step 4** Specify the SSH public key in Open SSH format.

```
switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
```

```
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

**Step 5** Save the configuration.

```
switch(config)# copy running-config startup-config
```

## Configuring X.509v3 Certificate-Based SSH Authentication

You can configure SSH authentication using X.509v3 certificates.

### Before you begin

Enable the SSH server on the remote device.

### SUMMARY STEPS

1. **configure terminal**
2. **username** *user-id* [**password** [0 | 5] *password*]
3. **username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**}
4. [**no**] **crypto ca trustpoint** *trustpoint*
5. [**no**] **crypto ca authentication** *trustpoint*
6. **crypto ca crl request** *trustpoint* **bootflash:static-crl.crl**
7. (Optional) **show crypto ca certificates**
8. (Optional) **show crypto ca crl** *trustpoint*
9. (Optional) **show user-account**
10. (Optional) **show users**
11. (Optional) **copy running-config startup-config**

### DETAILED STEPS

#### Procedure

|               | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                      |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre>                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                            |
| <b>Step 2</b> | <b>username</b> <i>user-id</i> [ <b>password</b> [0   5] <i>password</i> ]<br><br><b>Example:</b><br><pre>switch(config)# username jsmith password 4Ty18Rnt</pre> | Configures a user account. The <i>user-id</i> argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. Valid characters are uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, hyphen (-), period (.), underscore |

|               | Command or Action                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                                                                                                                                            | <p>( ), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames.</p> <p>Usernames must begin with an alphanumeric character.</p> <p>The default password is undefined. The <b>0</b> option indicates that the password is clear text, and the <b>5</b> option indicates that the password is encrypted. The default is <b>0</b> (clear text).</p> <p><b>Note</b><br/>If you do not specify a password, the user might not be able to log in to the Cisco NX-OS device.</p> <p><b>Note</b><br/>If you create a user account with the encrypted password option, the corresponding SNMP user will not be created.</p> |
| <b>Step 3</b> | <p><b>username</b> <i>user-id</i> <b>ssh-cert-dn</b> <i>dn-name</i> {<b>dsa</b>   <b>rsa</b>}</p> <p><b>Example:</b></p> <pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre> | Specifies an SSH X.509 certificate distinguished name and DSA or RSA algorithm to use for authentication for an existing user account. The distinguished name can be up to 512 characters and must follow the format shown in the examples. Make sure the email address and state are configured as emailAddress and ST, respectively.                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 4</b> | <p>[no] <b>crypto ca trustpoint</b> <i>trustpoint</i></p> <p><b>Example:</b></p> <pre>switch(config)# crypto ca trustpoint winca</pre>                                                                                                                                                                     | Configures a trustpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 5</b> | <p>[no] <b>crypto ca authentication</b> <i>trustpoint</i></p> <p><b>Example:</b></p> <pre>switch(config)# crypto ca authentication winca</pre>                                                                                                                                                             | Configures a certificate chain for the trustpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 6</b> | <p><b>crypto ca crl request</b> <i>trustpoint</i> <b>bootflash:static-crl.crl</b></p> <p><b>Example:</b></p> <pre>switch(config)# crypto ca crl request winca bootflash:crllist.crl</pre>                                                                                                                  | <p>Configures the certificate revocation list (CRL) for the trustpoint. The CRL file is a snapshot of the list of revoked certificates by the trustpoint. This static CRL list is manually copied to the device from the Certification Authority (CA).</p> <p><b>Note</b><br/>Static CRL is the only supported revocation check method.</p>                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 7</b> | <p>(Optional) <b>show crypto ca certificates</b></p> <p><b>Example:</b></p> <pre>switch(config)# show crypto ca certificates</pre>                                                                                                                                                                         | Displays the configured certificate chain and associated trustpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 8</b> | <p>(Optional) <b>show crypto ca crl</b> <i>trustpoint</i></p> <p><b>Example:</b></p> <pre>switch(config)# show crypto ca crl winca</pre>                                                                                                                                                                   | Displays the contents of the CRL list of the specified trustpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                | Command or Action                                                                                                                 | Purpose                                                        |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Step 9</b>  | (Optional) <b>show user-account</b><br><br><b>Example:</b><br>switch(config)# show user-account                                   | Displays configured user account details.                      |
| <b>Step 10</b> | (Optional) <b>show users</b><br><br><b>Example:</b><br>switch(config)# show users                                                 | Displays the users logged into the device.                     |
| <b>Step 11</b> | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config startup-config | Copies the running configuration to the startup configuration. |

## Configuration Example for X.509v3 Certificate-Based SSH Authentication

The following example shows how to configure SSH authentication using X.509v3 certificates:

```
configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
rsa
crypto ca trustpoint tp1
crypto ca authentication tp1
crypto ca crl request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crl tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /CN=SecDevCA
  Last Update: Aug 8 20:03:15 2016 GMT
  Next Update: Aug 16 08:23:15 2016 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A

show user-account
user:user1
  this user account has no expiry date
  roles:network-operator
  ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN =
```

```

user1; Algo: x509v3-sign-rsa

show users
NAME      LINE      TIME      IDLE      PID      COMMENT
user1     pts/1     Jul 27 18:43 00:03     18796    (10.10.10.1)  session=ssh

```

# Configuring Telnet

## Enabling the Telnet Server

By default, the Telnet server is enabled. You can disable the Telnet server on your Cisco Nexus device.

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **[no] feature telnet**

### DETAILED STEPS

#### Procedure

|               | Command or Action                          | Purpose                                                     |
|---------------|--------------------------------------------|-------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>          | Enters global configuration mode.                           |
| <b>Step 2</b> | switch(config)# <b>[no] feature telnet</b> | Enables/disables the Telnet server. The default is enabled. |

## Reenabling the Telnet Server

If the Telnet server on your Cisco Nexus device has been disabled, you can reenabling it.

### SUMMARY STEPS

1. switch(config)# **[no] feature telnet**

### DETAILED STEPS

#### Procedure

|               | Command or Action                          | Purpose                      |
|---------------|--------------------------------------------|------------------------------|
| <b>Step 1</b> | switch(config)# <b>[no] feature telnet</b> | Reenables the Telnet server. |

## Configuring the Telnet Source Interface

You can configure Telnet to use a specific interface.

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **ip telnet source-interface** *type slot/port*

**DETAILED STEPS****Procedure**

|               | <b>Command or Action</b>                                                | <b>Purpose</b>                                                                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>configure terminal</b>                                       | Enters global configuration mode.                                                                                                                                                                                                                                    |
| <b>Step 2</b> | switch(config)# <b>ip telnet source-interface</b> <i>type slot/port</i> | Configures the source interface for all Telnet packets. The following list contains the valid values for <i>interface</i> . <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> <li>• vlan</li> </ul> |

**Example**

This example shows how to configure the Telnet source interface:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip telnet source-interface ethernet 1/6
switch(config)# show ip telnet source-interface
VRF Name                Interface
default                  Ethernet1/6
switch(config)#
```

**Starting Telnet Sessions to Remote Devices**

Before you start a Telnet session to connect to remote devices, you should do the following:

- Obtain the hostname for the remote device and, if needed, obtain the username on the remote device.
- Enable the Telnet server on the Cisco Nexus device.
- Enable the Telnet server on the remote device.

**SUMMARY STEPS**

1. switch# **telnet** *hostname*



## DETAILED STEPS

### Procedure

|        | Command or Action                     | Purpose                                                                                                            |
|--------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>telnet</b> <i>hostname</i> | Creates a Telnet session to a remote device. The <i>hostname</i> argument can be an IPv4 address or a device name. |

### Example

The following example shows how to start a Telnet session to connect to a remote device:

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

## Clearing Telnet Sessions

You can clear Telnet sessions from the Cisco Nexus device.

### SUMMARY STEPS

1. switch# **show users**
2. switch# **clear line** *vtty-line*

### DETAILED STEPS

#### Procedure

|        | Command or Action                          | Purpose                            |
|--------|--------------------------------------------|------------------------------------|
| Step 1 | switch# <b>show users</b>                  | Displays user session information. |
| Step 2 | switch# <b>clear line</b> <i>vtty-line</i> | Clears a user Telnet session.      |

## Verifying the SSH and Telnet Configuration

To display the SSH configuration information, perform one of the following tasks:

| Command or Action                                                     | Purpose                   |
|-----------------------------------------------------------------------|---------------------------|
| switch# <b>show ssh key</b> [ <i>dsa</i>   <i>rsa</i> ][ <i>md5</i> ] | Displays SSH server keys. |

| Command or Action                                 | Purpose                                                                                                                                                  |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| switch# <b>show running-config security [all]</b> | Displays the SSH and user account configuration in the running configuration. The all keyword displays the default values for the SSH and user accounts. |
| switch# <b>show ssh server</b>                    | Displays the SSH server configuration.                                                                                                                   |
| switch# <b>show user-account</b>                  | Displays user account information.                                                                                                                       |
| switch# <b>show users</b>                         | Displays the users logged into the device.                                                                                                               |
| switch# <b>show crypto ca certificates</b>        | Displays the configured certificate chain and associated trustpoint for X.509v3 certificate-based SSH authentication.                                    |
| switch# <b>show crypto ca crl trustpoint</b>      | Displays the contents of the CRL list of the specified trustpoint for X.509v3 certificate-based SSH authentication.                                      |

## Default Settings for SSH

The following table lists the default settings for SSH parameters.

**Table 1: Default SSH Parameters**

| Parameters                  | Default                          |
|-----------------------------|----------------------------------|
| SSH server                  | Enabled                          |
| SSH server key              | RSA key generated with 1024 bits |
| RSA key bits for generation | 1024                             |
| Telnet server               | Enabled                          |